

## **The e-Borders Scheme**

Soon, when you go abroad you'll be forced to give the Government personal details such as:

- the contact numbers of all the places where you are staying
- the addresses of all the places you'll be staying at
- your vehicle number
- the number of the credit card you used to pay for your trip
- details of the other people in the party

and many other highly intrusive details.

### **Key Points**

- Travel histories for all passengers will be held on a central database for 10 years – creating a gigantic watch list on which we all appear as suspects
- Our private information will be shared with the Inland Revenue, Secret Services and other – unspecified – organisations

The data collected on us will be used to determine whether we are given a 'green' light to travel, 'yellow' (subject to extra checks) or red, in which case we will be refused boarding, detained or taken into custody. You will face – at the very least – long delays if there are any mistakes or questions regarding YOUR data.

Yet, unbelievably:

- There is NO standard system in place for gathering your data
- The checks will NOT reveal if a person is using a false identity
- People who have established a false – but unblemished – identity will travel with ease

## An overview

The Home Office claims e-Borders will "transform our border control" by gathering information on all travellers entering or leaving the country by air, sea or rail. To some extent they are right – but only in the sense that it will be for the worse, as the government continues in its desire to create the most intrusive surveillance state ever created.

Through the scheme, launched as a pilot called "Project Semaphore" in 2004, the Government has already started to compile biographical information on all travellers from the UK, with 53 pieces of intrusive advance information being obtained from carriers, such as airline and flight number, details of reservations and payment.

The Home Office will generate "travel histories" for all passengers, collecting our biometrics, including fingerprints, DNA, iris patterns and face recognition, some of which have already started to be contained in passports.

The e-Borders scheme began to go live in April, automatically generating details of an estimated 250 million journeys into and out of the UK each year, which will be stored on a central database for up to ten years at the database centre in Wythenshawe, Manchester. There are also plans to expand the use of biometric data and gather it as a key part of the e-Borders database. An iris recognition scheme is already in operation at Heathrow and several other airports around the country.

The Home Office also says it has the right to share information from this database with other unspecified organisations where *"necessary ... to enable them to carry out their functions"*.

In a report for the Institute for Public Policy Research, Frank Gregory, professor of European Security at the University of Southampton, warned that it will be possible to fool the system.

The report said:

*"There are two key problems with the e-Borders programme. First, it will not reveal if the person matching the identity documents has created a false identity and, second, 'watchlist' scrutiny only works if a suspect person continues to use a 'flagged' name."*

Chris Grayling MP, described his concerns regarding e-Borders:

*"The justification is always about security or personal protection. But the truth is that we have a government that just can't be trusted over these highly sensitive issues. We must not allow ourselves to become a Big Brother society."*

## Scheme Details

The UK e-Borders scheme is way ahead of the measures being operated by the other countries in the EU and the USA.

The USA planned to introduce a profiling system (CAPPS II) for all passengers, but it was withdrawn after a damning report from the General Accountability Office (GAO) and opposition from civil liberties groups. It is being replaced by a straightforward watch-list monitoring programme, that is, checking all passengers against a list of around 125,000 people.

Included in the EU plans that were agreed in April 2004, are the mandatory collection of Passenger Name Records (PNR) and biometrics (eg: finger-prints) in visas and passports (introducing fingerprints on EU ID cards). But there is, as yet, no overall plan for how each of the 25 member states will use the data collected.

The UK's "e-Borders Programme" is intended to be a comprehensive system with the mandatory collection of data and biometrics for everyone who enters and leaves the country. It will build on new powers in the Immigration and Nationality Act and some of its implications are given in a "Partial Regulatory Impact Assessment on data capture and sharing powers for the border agencies" (RIA).

## What We Will Face

The e-Borders system's original "purposes", the countering of terrorism and organised crime, have been rapidly expanded. The system is no longer just needed for "terrorism and organised crime" but "to support general police and criminal justice functions" (RIA)

The overall "Objectives" are set out as:

1. The "ability to deny travel"
2. "Assessing in advance of arrival [of] the immigration and security threats posed by passengers"
3. To share information between immigration, police, security and intelligence agencies
4. To use "passenger information" and intelligence to inform the agencies.

Agencies will capture passenger data through a "single window" and jointly analyse "bulk data" – whilst retaining the data for up to 10 years. The immigration, police and security agencies already have powers to require carriers (air, sea and land) to provide information of people travelling to the UK and in some cases from the UK (ie: to the USA).

However, the decision to "share or disclose information must be considered on a "case-by-case" basis" where the agencies can rely on "certain information processing exemptions" under the 1988 Data Protection Act " but again, this is on a "case-by-case" basis". Nowhere is it spelt out how data protection is going to work when the agencies hoover-up the data on every movement, add comments to some entries, or pass it to any foreign law enforcement agency

The e-Borders programme has moved into the second of its three stages, mapped out between 2004-2014 which include the "Iris Recognition Immigration System" for automated entry controls using biometrics, the e-Borders Operations Centre (e-BOC) authorising "Authority to Carry" which will "roll out incrementally to all air, sea and rail carriers operating internationally to/from all major UK ports". So, effectively the government is not targeting suspects' information, but is seeking to "capture" data on everyone entering or leaving the UK, treating us all as suspects on a single gigantic watch list.

The UK is setting up the equivalent of the "US Visit programme" which keeps a historical record on all entrants. Passenger information, or PNR (Passenger Name Record) is provided when a person books a ticket. This is to be supplemented by Advanced Passenger Information (API) whereby

airlines flying to the UK will have to install passport readers at check-in desks and supply a list of those actually travelling to the agencies. The cost of this will be passed onto passengers by the carriers.

The PNR and API schemes are to be supplemented by the "Authority to carry" (ATC) scheme are "geared to the perceived risk" by: "An authority to carry (ATC) scheme will allow the Immigration Service to prevent specified categories of passenger from travelling to the UK by requiring carriers to request a check against government databases before departure."

## Profiling

"The Border Agencies will make use of profiling which involves running a series of pre-defined profiles against reservation data. Most profiles are based on information obtained from actual results or from intelligence received"

Under another new scheme 'low risk' passengers will "qualify for faster clearance" which will be open to UK citizens, those permanently or temporarily resident, visa-holders and "frequent visitors who meet certain criteria" for whom:

*"There will be a one-off enrolment process, for those wishing to use the system. When they subsequently arrive at any of the UK ports with IRIS barriers, they will bypass the queues to see an immigration officer and look into a camera. If the system recognises them as being admissible, a barrier will open automatically and let them into the UK. Use of the IRIS barriers may be extended in the future to holders of biometrically-enabled travel documents, without the need to preregister."*

This raises a number of questions.

1. If a person is not a suspect then they will pass through the whole system with ease, both those who do so legitimately and those not known to or being targeted by the agencies.
2. People who have established a false, unblemished, identity will also pass through.
3. As the "IRIS barriers" become established at all points of entry those who do not have biometric passports or choose not to give the state yet another personal biometric may find their "profile" records this fact.
4. The whole system depends on "profiles", whose content is undefined and may be extended to new categories depending on the climate of "fear".

## Tracking and Tracing All Our Movements

New mandatory powers have been given to customs, police and immigration agencies for the provision of passenger data in advance of arrival for journeys to and from third countries (non-EU) and to and from EU countries by carriers.

This will allow

*"sufficient time for the information to be used for profiling and targeting of individuals of potential interest, and allow time for a decision to be made as to whether an intervention is appropriate"*

Targeting will not only look at individuals and their "patterns of travel" but also at "high risk flights", that is, flights to countries like Pakistan. The Immigration Service will have extended powers to request additional Advanced Passenger Information (API) biometric data from travel documents and "additional reservation data to the extent that it is known to the carrier".

## Checking biometric data

The EU Directive on passenger information will require carriers to provide this data in advance of departure - this is to allow a suspected person to be detained before travelling.

Everyone arriving will be subject to these checks - UK residents, EU residents and non-EU people. The check will involve the taking of a biometric "on the spot" to check against the biometric held on the chip in a travel document. We already have the ability to hold a digitised image of the normal passport photo, and finger-prints.

These new powers mean that an immigration official will

- Access the information held on the "chip" of all those who have chips in their passports/travel documents
- Check that the data relates to the person presenting the document.

(EU nationals and all other third country nationals arriving will be required to "provide biometric information" which can be compared with the information held on the document presented - this will be a "one-to-one" check involving the mandatory taking of a biometric if the travel document contains one. That is until an EU-wide database is set up to conduct "one-to-many" checks. For British citizens it will mean comparing the biometric information provided against that contained in the passport or contained in the National Identity Register)

## UK "roll-out"

The UK's "e-Borders" system will, when fully implemented, be one of the most comprehensive in the world... and potentially the most intrusive.

The roll-out is dependent on a host of other schemes, including biometric passports which started in 2006; registration on the IRIS automated entry system. The final stage can only be reached when all UK residents will, in theory, have biometric passports around about 2018.

So from now until 2018, the intermediate stage, there will be a confusion of different queues at border control points, formed by:

1. Those using the automated entry IRIS scheme
2. Those with biometric passports/ID cards from the UK (allowing "one-to-one" and "one-to-many" checks) and from other EU countries (allowing "one-to-one" but not "one-to-many" checks until there is an EU-wide database)
3. Those with biometric passports from non-EU countries (allowing "one-to-one" but not "one-to-many" checks)
4. Those with biometric visas issued by the UK/EU (if the "collision" of chips whereby an EU visa chip would clash with a national e-passport chip is resolved; then checked against the Visa Information System, VIS)
5. Those with "old-fashioned" passports from UK/EU
6. Those with "old-fashioned" passports from non-EU countries with biometrically "chipped" visas in their passports IF third countries agree to this. All that every country is obliged to put in their passports under the ICAO standard (International Civil Aviation Organisation) is simply a digitised image of the usual passport picture inserted onto a readable chip - this is not a biometric and does not require any "enrolment" by the individual.

## Joining It All Together

There are many stages in setting up such a system

1. The biometrics have to be collected (through so-called "enrolment") and the biometrics and personal data linked and stored on a central database.
2. "Readers" have to be installed at every point of departure (ie: at all check-in desks for all airlines flying to the UK/EU from anywhere in the world).

3. The mass of data has to be checked against "watch-lists" held by the receiving country's agencies and decisions taken on whether to "authorise" travel.

Those given a "green light" will be able to travel, those given a "yellow" would be subject to extra checks before boarding or placed under surveillance on arrival, and those given a "red" will be refused boarding, be detained or taken into custody. The "yellow" category is the most problematic, as this could be because a person is wrongly identified as a potential suspect.

It might be thought that having taken the decision in 2004 to introduce biometrics onto EU passports a standard system for gathering and checking the data would be in place too, or at least planned. However, it is apparent from a questionnaire sent out from the UK Presidency of the Council of the European Union that *a great variety of systems could be in place* (Note from UK Presidency: Reading systems for biometric e-Passports at EU border control points, EU doc no: 10559/04,1.7.05).

Discussions to create an EU (passenger name record) system are underway. In June 2008 the Council threw the Commission proposal out and in the autumn it will draw up its own draft. A number of governments do not like limiting the use of data to terrorism and organised crime and want to extend the proposal's scope from just in and out of the EU to travel between EU states and even within each state. The same view also supports extending the scope from air travel to land and sea travel too. An EU entry-exit system is planned for third country nationals entering with visas, and those without visas too, as is an EU version of an Electronic System for Travel Authorisation (ESTA). The former proposal includes the automated checking of EU citizens - that is, passports and biometrics (finger-prints) to be checked by "machines" not people. The EU-PNR exit-entry system and ESTA will put the EU on the same footing as the USA. The Prüm Treaty, agreed by 17 EU member states, has led to the incorporation of the policing aspects into EU law (the automated exchange of DNA, fingerprint and vehicle data) thus applying across all 27 member states. The immigration aspects - including the use of air marshals - are being adopted by the signatory states.

Further detail of future developments here - <http://www.statewatch.org/analyses/the-shape-of-things-to-come.pdf>

## What is the point?

The UK e-Borders system signals a shift from "targeting" suspected individuals to placing *everyone's* movements under surveillance.

This raises a whole range of privacy and data protection issues. This is especially as the scope of the system which although presented as necessary for countering terrorism and serious organised crime, is now being extended to cover all crime or all suspected crime, however minor. Equally, the "profiling" of an individuals' travel habits or individuals going to or from certain countries raises serious concerns that certain groups (eg: young men) and nationalities (northern African, Middle eastern or from Pakistan) will be targeted and subjected to extra checks and surveillance.

The value of the system's product to counter terrorism is flawed even after the full biometric roll-out in 2018.

**Our World Our Say**  
July 2009

*Many thanks to Statewatch in the compilation of this guide*